REMARKS/ARGUMENTS

Upon entry of this amendment, which amends claims 10-20, 26-27, 30-32, and 35-37 and cancels claims 1-9, 21-24, 28-29, and 33-34, claims 10-20, 26-27, 30-32, and 35-37 will be pending. Claims 1-9, 28-39, and 33-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shoup et al. ("Securing Threshold Cryptosystems against Chosen Ciphertext Attack", hereinafter "Shoup") and further in view of Schneier ("Applied Cryptography", hereinafter "Schneier"). Claims 10-19, 30-31, and 35-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Shoup et al. and Schneier system and further in view of Graunke et al. (US Patent No. 5,991,399, hereinafter "Graunke"). Claims 20-24, 32, and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shoup et al. further in view of Schneier. Claims 25-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Shoup et al. and Schneier, and further in view of Shamir ("How to Share a Secret", hereinafter "Sharmir"). Applicants respectfully request reconsideration of the claims in view of the amendments above and remarks below.

Claims 10-14

Claim 10 was rejected under 35 U.S.C. §103(a) as being unpatentable over Shoup and Schneier and further in view of Graunke. Claim 11 recites:

> generating and storing a database of $\binom{n}{k}$ values, where each value is the product of d and a unique k of the d_i numbers for $1 \le i \le n$, wherein each value is associated with a unique combination of k secret owners of the n secret owners;
>
> ...
>
> receiving k secret owner values from a unique combination of k secret owners;
>
> determining a value c that is associated with the unique combination; and
>
> determining the secret S using the value c and the k secret owner values.

Applicants have clarified the element of generating and storing a database of $\binom{n}{k}$ values. As claimed, each value is associated with a unique combination of k secret owners of the n secret owners. Different combinations of k secret owners may return the secret owner pieces. For example, if n=4 and k=3, then different combination of k secret owners may include owners #1, #2, and #3; owners #1, #2, and #4; owners #2, #3, and #4, etc. A value for each of the unique combinations of k secret owners is stored in the database. As claimed, when k secret owner values from a combination of k secret owners are received, a value c is determined that is associated with unique combination from the database. For example, if secret owner values are received from owners #1, #2, and #3, a value c for that combination is retrieved. The secret S is then determined using the value c and the k secret owner values.

Shoup, Schneier and Graunke do not disclose or suggest the above concept, as claimed. The rejection stated Shoup and Schneier failed to disclose or suggest generating and storing a database for the product of d and a unique number of the d_i's (part of the keys). However, the rejection stated that Graunke teaches storing a key in a database. Graunke discloses storing an asymmetric public key in a secure database. See *Graunke*, col. 7, lines 64-66. The asymmetric public key in Graunke does not disclose or suggest values that are associated with unique combinations of k secret owners of n secret owners. Rather, the asymmetric public key corresponds to a private key.

Further, Shoup, Schneier, and Graunke, either alone or in combination, do not disclose or suggest receiving k secret owner values from a combination of k secret owners and determining a value c from the database that is associated with that unique combination. The secret S, as claimed, is then determined based on the value c and the k secret owner values. Accordingly, Applicants respectfully request withdrawal of the rejection of claim 10.

Claims 11-14 depend from claim 10 and thus derive patentability at least therefrom. These claims also recite additional novel and non-obvious features. For example, claim 14 recites after the k secret owner pieces are received, the value c is retrieved from the database and S^c mod N is computed and S' is replaced with S^c mod N. Thus, as recited in claims 11-13, when a secret owner piece is received, S^q mod N is computed and S' is replaced with S^q

mod N until the k secret owner pieces have been received and the value c is used to compute S^c mod N to determine the secret S.

Claims 15-20, 26-27, 30-32, and 35-37

Applicants submit claims 15-20, 26-27, 30-32, and 35-37 should be allowable for at least a similar rationale as discussed with respect to claims 10-14. Accordingly, applicants respectfully request withdrawal of the rejections.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 415-576-0200.

Respectfully submitted,

Dated: 9/8/05

Brian N. Young
Reg. No. 48,602

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 415-576-0200
Fax: 415-576-0300
BNY:jtc
60582083 v1